Examination 1
Computer and Network Security
24 October, 1997

Instructions:

- Do not start the examination until instructed to do so.
- This test is closed book, but you may use one 8.5" by 11" sheet of notes you have prepared.
- Answer any three (3) questions below.
- Start the answer to each question on a new page (i.e., do **not** put the answer to more than one question on the same page).
- Show your work.
- Assemble your answers in numerical order of the questions when you submit them.
- **Leave a 1" square in the upper left corner for a staple.**
- Be sure to include your name on your answer sheets.
- You have 50 minutes to complete this examination.
- **Read and sign the following statement.** You may write this on your exam and sign it there if you wish to take the exam questions home with you today. Do not discuss this exam with anyone in this course who has not yet taken this exam.

On my honor, I have neither given nor received unauthorized aid on this examination, and I will not discuss the contents of this examination with any student who has not yet taken this examination.

Signed:

1. (a) What is a control? What are some of the types of costs of a control? Give examples of at least three types of costs. How do these costs relate to the effectiveness of a control? How does one determine whether a control should be used or not?
   (b) What are the three main goals of information security? In what ways do they compete with each other? In what ways do they complement each other?
   (c) (Grads) What is the Principle of Easiest Penetration? How does it relate to the nature of controls employed? Is there another principle you can derive from this? Explain.
2. (a) How are the programmed threats of virus, bacterium (or rabbit), and worm similar? How are they different? Do they have fundamentally different capabilities in terms of the damage they can do in a system? Explain.
   (b) What are the differences between a standard application program virus, a boot sector virus, and a macro virus? How difficult is it to detect each? How hard is it to eliminate each? How easy is it for each to spread?
   (c) (Grads) What steps could you take to prevent the spread of each of the types of virus mentioned above? What steps would be effective in eliminating each of these types of virus from an infected system?
3. (a) How does reusability affect security?
   (b) How does configuration management affect security?
   (c) How does modular design affect security?
   (d) (Grads) What are the limitations on the increased assurance one might hope for from modular design?
4. (a) What is isolation? Why is it important? What mechanisms exist to provide isolation? How do they work? What weaknesses do they have?
   (b) What is a capability? What properties must a capability have to be secure? When are capabilities most desirable? Give an example of how a capability might be used.
   (c) What are the three basic types of authentication? Give examples of each. What are their strengths and weaknesses?
   (d) (Grads) What is strong authentication and what is weak authentication? How do they relate to the three basic types of authentication mentioned above?
5. (a) Distinguish MAC and DAC.
   (b) How are they related to the TCSEC certification levels?
   (c) How did the German Green Book improve upon the Orange Book?
   (d) (Grads) Compare the Bell-LaPadula and the Biba security models. How do they relate to lattice-based security models?
6. (a) Distinguish database integrity, element integrity and element accuracy.
   (b) What is two-phase commit (two-phase update)? How is it related to security?
   (c) What is an inference attack? Name and describe three types of inference attack.
   (d) (Grads) What controls are used against inference attacks on databases? How do they work? Compare them.